

Mercer University School of Medicine – Student Email Policy

Purpose & Authority

The Mercer University School of Medicine Student Email Policy as approved by the MUSM IT Steering Committee is that **the MUSM email system is the approved channel for students for MUSM-related email communications**. This policy is to be considered subordinate to the *Mercer University Computer Facilities Access and Use Policy*.¹ Any discrepancy between this document and the *Mercer University Computer Facilities Access and Use Policy* shall be governed by to the *Mercer University Computer Facilities Access and Use Policy*.

Application

This policy applies to all students in the School of Medicine, the MPH program, or the MFS/MFT program while they are actively enrolled.

Review

This policy shall be reviewed periodically by the MUSM IT Steering Committee.

Provisions

- All students actively enrolled in the School of Medicine, the MPH program, or the MFS/MFT program will have an email account created for them on the MUSM electronic mail system. This account will be created on the MED email server (accounts will end in “@med.mercer.edu”), maintained by Medical Library Technical Staff.
- ALL OFFICIAL CORRESPONDENCE FROM MERCER FACULTY, STAFF, STUDENTS, AND ADMINISTRATION SHALL BE DIRECTED TO THESE ACCOUNTS.
- All students are responsible for checking their MED accounts regularly.
- MED accounts will not be forwarded to any external email account for any student.
- Each student’s email accounts will be maintained for 90 days beyond his/her graduation date. If a student leaves the University for any other reason, the email account will be terminated immediately.

Approved Use

The MUSM electronic mail system is to be used for administrative and educational purposes only. The e-mail system is not to be used for personal communication, for-profit, or commercial purposes. Students are prohibited from using the e-mail system for mass mailings which are not directly related to MUSM business or MUSM-sponsored events. This restriction includes but is not limited to SPAM (unsolicited commercial advertising distributed by e-mail,) mail bombing, pyramid schemes, and chain letters.

Monitoring

E-mail content is not monitored by systems or network administrators unless they have been directed to do so by the appropriate University authority. Monitoring will only be performed if required as part of the investigative process. In such an event, e-mail messages may be copied or locked to prevent loss of material that may be used as evidence.

Remedies

The Medical Library System Administrator may temporarily disable a student account if necessary to protect the security of the email system. The MUSM Dean’s Office must approve any permanent loss of use of email facilities for a student. Permanent loss of use may result from any deliberate attempt to misuse or damage MUSM email systems, or failure to comply with Mercer University or MUSM policies for use of Mercer University computer system.

Last Reviewed: December 2001

*Please direct questions/comments to the Mercer University Medical Library Systems Librarian:
mccarley_lr@mercercer.edu or 301-2151.*

¹ Attached to this document; also available online <http://www.mercer.edu/acadcomp/ComputerLabs/CFAAUPOL.HTML>

Mercer University Computer Facilities Access and Use Policy

PURPOSE

The purpose of this document is to define appropriate and acceptable uses as well as certain inappropriate and unacceptable uses of the University's computer facilities and networks. It will further serve to educate authorized users about their responsibilities when using these facilities. Many of the regulations herein simply restate obligations that follow from other existing University policies or laws.

DEFINITIONS

"University computers and network facilities" comprise all computers owned or administered by any part of Mercer University at any of its locations or connected to the University's communications facilities. "Authorized use" is permission granted by the appropriate part of the University's governance and/or management structure and depends on the particular computers and/or network facilities involved and how they are administered.

APPROPRIATE USE

Mercer University maintains computer facilities for administrative and educational purposes only. These facilities may not be used for any commercial purpose. The computer facilities in academic areas are designed primarily for preparation of classroom assignments. Theft, failure to observe copyright laws, and/or tampering with any computer system or network will place violators in jeopardy of loss of privileges as well as prosecution through law enforcement and University agencies. All cases will be referred to the appropriate University agency.

Personal computers and workstations are intended for use as "clients" that request computing services rather than "servers" that provide computing services. Providing services to other users, such as other Mercer network users or the Internet at large, potentially consumes excessive amounts of network bandwidth and compromises network security. Without explicit authorization from the Associate Vice President of Technical Services, computers shall not be configured to operate as servers, including but not limited to file, print, mail, web, chat, media streaming, name, time, directory, quote, network management, or proxy servers. Any computer ostensibly configured as a client but running special software that essentially provides services to other users is regarded as being a server and deemed to be in violation of this policy. Specific examples of software or services that are prohibited without authorization are Napster and Gnutella, both of which are used to share files between computers on a network or the Internet.

AUTHORIZED USERS

Open-Access Computer Labs

All currently enrolled full-time and part-time students, full-time or part-time faculty, and staff are permitted to use the open-access computer facilities on a first-come, first-served basis or by prior arrangement with the facility staff. Open-access computer facilities are staffed by student assistants for the convenience of our users. They are trained to assist users with questions and to help with hardware and software problems, but they are not permitted to do homework for other students. Student assistants are authorized to enforce the rules related to access and use of computer facilities.

Academic Departments

Several academic departments provide computer facilities for student use. Some are open-access labs, and others are reserved for students in particular disciplines. These departments may have their own policies and guidelines for access and use of their facilities.

Administrative Departments

Various administrative departments maintain responsibility for access and use of administrative and academic computer systems. These departments grant access to the appropriate users and may have additional policies and guidelines for access and use of these systems.

USER RESPONSIBILITIES AND GUIDELINES FOR COMPUTER ACCESS

The computer equipment, facilities, and services of the University are shared resources available to all currently enrolled students, faculty and staff. Despite safeguards, these resources can be used improperly. We need the cooperation of our users to minimize improper use or abuse of these facilities. We have established the following guidelines to help us provide the best possible service to all our users.

Users are required to register when using open-access computer facilities and must present a valid Mercer University identification when requested.

A valid user account is required for access to some computers and networks. Users should access only accounts which they are authorized to use and should use those accounts only for authorized purposes in accordance with established policies and guidelines. Authorized users should not share their passwords or user IDs with others.

Users should not attempt to modify hardware or software or subvert account restrictions on any computer system or network.

Users should respect the rights of others to privacy and intellectual property rights and refrain from unauthorized access or copying.

Users should refrain from recreational use of computers and networks during peak hours.

Users should make economical and wise use of resources.

Users should report suspected unauthorized use of resources to the computer lab staff immediately.

Unauthorized use of computer equipment will have serious consequences and may result in suspension or dismissal from Mercer. Unauthorized use may also constitute grounds for civil action for restitution or criminal prosecution.

USE OF COMPUTER SOFTWARE

Mercer University licenses the use of computer software from a variety of outside companies. Mercer does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.

Mercer faculty, staff, and students shall use software only in accordance with license agreements.

Mercer employees learning of any misuse of software or related documentation within the University shall notify the appropriate staff or Mercer University's legal counsel.

Anyone who makes, acquires or uses unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include dismissal.

INTERNET ACCESS

Mercer University's network, BearNet, provides access to the Internet and exists for the primary purpose of providing faculty, staff, and students with the necessary tools to communicate with colleagues and to obtain and exchange information for educational and research purposes. The GaIN (Georgia Interactive Network for Medical Information) network provides Internet access for its members through Mercer's BearNet. Accounts provided through the GaIN network are subject to Mercer University's Internet Acceptable Use Policy as well as GaIN's Internet Access Policy. Any use of BearNet, the Internet and/or connecting networks for commercial, private or for-profit purposes is prohibited.

Transmission of any material over these networks in violation of any U.S. or state laws or regulations is prohibited. Users of Mercer's BearNet are expected to be responsible in their use of the network and should avoid actions that interfere with the work of others on the network. Mercer University's BearNet is connected to many other networks worldwide; therefore, BearNet users must observe the acceptable use policy of any other network accessed through BearNet. Mercer University does not own nor control any of the various facilities and communications lines through which network access is provided outside the Mercer network. Other networks may have special usage policies which may be obtained from those network providers.

"...The University is guided by the historic principles of religious and intellectual freedom, while affirming religious and moral values that arise from the Judaeo-Christian understanding of the world." (University Mission Statement) In keeping with the University Mission Statement, the University does not condone the use of University electronic resources for accessing, viewing, or downloading textual or graphic materials that are pornographic or otherwise sexually explicit in nature.

E-Mail

Mercer University's electronic mail system is to be used for administrative and educational purposes only. The e-mail system is not to be used for personal communication, for-profit, or commercial purposes. Students, faculty, and staff are prohibited from using the e-mail system for mass mailings which are not directly related to Mercer business or Mercer-sponsored events. This restriction includes but is not limited to SPAM (unsolicited commercial advertising distributed by e-mail,) mail bombing, pyramid schemes, and chain letters.

E-mail content is not monitored by systems or network administrators unless they have been directed to do so by the appropriate University authority. Monitoring will only be performed if required as part of the investigative process. In such an event, e-mail messages may be copied or locked to prevent loss of material which may be used as evidence.